Register now for your free, tailored, daily legal newsfeed service.

Find out more about Lexology or get in touch by visiting our **About** page.

Indian regulatory environment & judicial proactiveness in tackling child sexual abuse content

Nishith Desai Associates

India | April 25 2025

Factual Background

The rise in the proliferation of child sexual exploitation and abuse material ("**CSEAM**") on intermediary platforms represents a grave menace with far-reaching consequences for individuals, communities, and digital ecosystems worldwide. In 2015, an NGO named Prajwala submitted a letter to the Supreme Court expressing concern over videos depicting sexual violence involving children being circulated on the internet. On the basis of this, the Court directed that a committee be constituted to advise the Court "on the feasibility of ensuring that videos depicting rape, gang rape and child pornography are not available for circulation." The Committee issued various recommendations pursuant to which the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules**") were issued to address the concerns relating to CSEAM.

The National Commission for Protection of Child Rights ("**NCPCR**") has also undertaken various measures, including issuance of *suo moto* notices, holding awareness programs and issuing takedown requests, to check the proliferation of CSEAM along with issuing a set of recommendations to prevent the distribution of CSEAM, display of disclaimers, parental consent etc.

In addition, the Central Government in 2024 launched an online portal, known as SAHYOG, to automate the process of issuing takedown orders to intermediaries under Section 79(3)(b) of the Information Technology Act, 2000 ("**IT Act**"). The Indian Cyber Crime Coordination Centre (I4C) conducted a meeting on January 30, 2025, with various social media platforms in relation to CSEAM reporting and as per reports, the SAHYOG portal would act as a one-stop platform for reporting CSEAM, which would redirect reports to authorized law enforcement agencies.

However, the portal is the subject of a constitutional challenge before the Karnataka High Court. The challenge is centered on the use of the portal as a parallel takedown process bypassing the procedural requirements for issue of takedown orders as per Section 69A of the IT Act read with the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

Recently, the Ministry of Electronics and Information Technology ("**MeitY**") held a meeting on February 19, 2025, with social media platforms, the National Human Rights Commission ("**NHRC**"), in relation to the reporting of CSEAM. MeitY had asked social media platforms to submit a status-cum-action taken report on tackling CSEAM, which will be forwarded to the NHRC, which is expected to present its findings on the same to a parliamentary committee for further deliberations. The meeting is following a landmark Supreme Court judgement dated September 23, 2024 ("**Just Rights Case**"), which inter alia dealt with the obligation of intermediary platforms to report CSEAM to the local police or the Special Juvenile Police Unit (SJPU) as per the Protection of Children from Sexual Offences Act, 2012 ("**POCSO**") and rules thereunder.

In its judgement, the Supreme Court of India clarified several major points on the interpretation of provisions relating to CSEAM under the IT Act and POCSO.

Given the divergent views of various State High Courts, the Court's interpretation explicitly clarifies that there is no requirement for actual sharing or transmission of CSEAM, and mere possession or storage of CSEAM may be sufficient to trigger certain provisions.

The Court also set out several crucial observations on the proliferation of CSEAM and its impact on the cycle of exploitation of children, reporting obligations of intermediary platforms, and the role of organizations like the NCPCR in monitoring such content.

Provisions	Prohibited Content	Prohibited Actions
Section 67	Any material, in electronic form, which is lascivious or appeals to the prurient interest, or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it	Publishing, transmitting or causing to be published or transmitted
Section 67A	Any material, in electronic form, which contains sexually explicit act or conduct	Publishing, transmitting or causing to be published or transmitted
Section 67B(a)	Any material, in electronic form, which depicts children engaged in sexually explicit act or conduct	Publishing, transmitting or causing to be published or transmitted
Section 67B(b)	Any material, in electronic form, depicting children in obscene or indecent or sexually explicit manner	Creating, collecting, seeking, browsing, downloading, exchanging or distributing

Section 294 of the Bharatiya Nyaya Sanhita, 2023 ("**BNS**") in relation to obscenity prohibits the distribution, public exhibition or putting into circulation, in any manner, obscene objects (which includes writing, drawing, representation, figure or content in electronic form) and even taking part in or receiving profits from any business in the course of which the person knows or has reasons to believe that an obscene object is made for certain prohibited purposes.

Judgement of the Court

(a) Interpretation of Section 15 of POCSO

The Court noted the different views of various High Courts on the interpretation of Section 15 of the POCSO and Section 67B of the IT Act. Section 15 of POCSO prohibits storage or possession of pornographic material involving a child, which are not deleted, destroyed or reported, amongst others. Against this background, the Court interpreted Section 15 of POCSO and Section 67B of IT Act.

i. Mere possession or storage of child pornographic material may trigger Section 15 of POCSO

The Court noted that Section 15 of POCSO deals with inchoate offences, or undeveloped or incomplete offences, i.e., acts that are committed in preparation of a further offence. It seeks to penalize acts where a preparatory step is conducted towards more significant criminal conduct. This allows intervention at an early stage, acts as deterrent to more serious offences and reflects societal interest in preventing accumulation/availability of CSEAM.

Hence, there is no requirement for actual transmission or sharing to attract any of the sub-sections of Section 15 of POCSO. Mere storage or possession of CSEAM with the specific intent would trigger the offence under Section 15.

Section 15 penalizes three different forms of storage / possession of child pornography when carried out with specific intent / purpose.

1. Section 15(1) penalizes an omission to delete, destroy or report CSEAM by a person storing or possessing child pornographic content. For Section 15(1), there must be a specific intent demonstrable from the attending circumstances attributable to the failure to delete, destroy or report, indicating intention to share or transmit the material.
2. Section 15(2) penalizes the storage or possession of CSEAM material in order to ***facilitate*** the transmission, propagation, display or distribution of CSEAM. For Section 15(2), facilitation can be shown through any form of preparation or setup done that would enable that person to transmit it or to display the material.
3. Section 15(3) penalizes the storage or possession of child pornographic material when done for a commercial purpose, commercial purpose was interpreted to encompass any activity or transaction that is carried out or undertaken as a means of any commercial enterprise i.e., with the object or intention of any gain, irrespective of whether it was in monetary terms or not.

Accordingly, it is the preparation and *intention* to commit the crime which is being punished and not the commission of any criminal act in the traditional sense.

ii. Meaning of 'possession' under Section 15 of POCSO

The Court observed that persons were attempting to circumvent the application of the terms "storage" or "possession" under Section 15 of POCSO by refraining from actually downloading CSEAM and instead distributing links to posts on social media containing CSEAM. While these mechanisms were undertaken to bypass the language of "storage" of CSEAM, the word "possession" which was inserted vide 2019 amendment to POCSO would include constructive possession. Constructive possession was held to mean possession beyond physical control including situations where an individual had the power to control, even without physical possession. Hence, if an individual indulged in viewing, distributing or displaying CSEAM without actually possessing or storing it in any device or in any form or manner, it would still amount to 'possession' if the person exercised an invariable degree of control over such material.

This was to ensure that persons cannot escape liability by distancing themselves from physical possession of CSEAM while retaining the ability to control it.

The Court also held that the offence of 'storage' or 'possession' may still be triggered if an offender deleted the data subsequent to viewing it. There was no requirement for the storage or possession to exist at the time of registration of FIR or any criminal proceedings, as Section 15 is not fixated on any particular time frame.

iii. Meaning of 'child pornography' under POCSO

Section 15 also required that the material in question involved a 'child' and amounted to 'child pornography,' to attract the offence.

The Court held that the definition of "child pornography" under Section 2(da) of POCSO meant any visual depiction of a child involved in any sexually explicit conduct, including photographs, videos, etc., which *appear to depict a child.*

The Court has interpreted this to mean a subjective test or criteria to ascertain whether the visual depiction at hand appears to depict a child. If an ordinary person of a prudent mind would reasonably believe to *prima facie* depict a child or appear to involve a child, it would be deemed as 'child pornography'. This can be undertaken through a forensic science laboratory, expert opinion, or even the assessment of such material by courts themselves, depending on the facts of the case.

iv. Presumption of culpable mental state under POCSO

In cases of offences under POCSO requiring a culpable mental state, the POCSO permits the court to presume the existence of such a mental state. The Court clarified that this provision exists because it is difficult to look into the mind of the accused and determine their intention for doing a particular act, especially in cases of inchoate offences of a clandestine nature. Such presumption can be rebutted by the accused either by discrediting the prosecution's case or by leading evidence to prove the contrary, beyond a reasonable doubt.

The Court held that the presumption is only triggered when the prosecution is able to establish the foundational facts necessary to constitute the particular offence. These foundational facts typically involve proving the facts or elements relating to the actus reus of the offence. For Section 15(1), the foundational fact would *simpliciter* be the storage or possession of CSEAM and the failure to delete, destroy or report the same. For Section 15(2), in addition to the factum of storage or possession, it would also require any other material to indicate any actual transmission, or any form of an overt act such as preparation or setup done for the facilitation of the transmission of CSEAM. Similarly, for Section 15(3), it would require proof of the additional element to indicate that the storage or possession had been done for some gain or benefit or the expectation of the same.

v. Scope of Section 67B of the IT Act

The Court interpreted Section 67B of the IT Act and held that it not only punishes the electronic dissemination of child pornographic material, but also the creation, possession, propagation and consumption of such material as-well as the different types of direct and indirect acts of online sexual denigration and exploitation of the vulnerable age of children.

The Court relied upon its earlier order in *Sharat Babu Digumarti v. Govt. of NCT of Delhi* in which case the court held that Section(s) 67 – 67B were a complete code when it came to offences relating to electronic forms of obscene and pornographic material. Given this, these provisions ought to be interpreted in a purposive manner that suppresses the mischief and advances the intent of the provision.

Other Observations of the Supreme Court

In addition to the above, the Court emphasized the need for strict action against those involved in producing, distributing, or consuming CSEAM. Additionally, it observed that the NCPCR must go beyond the letter of its empowering provisions under the POCSO and address the practical challenges in combating child abuse, exploitation, and addiction to pornography.

(a) Intermediaries' duties relating to CSEAM

The Court also reiterated the importance of reporting obligations under Section 19 of POCSO. It mandated that any person who apprehends or has knowledge of an offence under POCSO must report it to the Special Juvenile Police Unit or local police and failure to do so is punishable up to six months of imprisonment, a fine, or both. Additionally, employers or supervisors who fail to report offences committed by subordinates can face imprisonment of up to one year and fines. By citing various cases, the Court also underscored that reporting is the foundation of POCSO, enabling prompt investigations and arrests, and urged against leniency in punishing failures to report under POCSO.

Further, the Court also discussed the role of intermediary platforms in checking the proliferation of child pornography pursuant to their due diligence obligations under the IT Act and the IT Rules in order to preserve their 'safe harbour' from liability for content on their platform. The Court referenced Section 79(3) of the IT Act, which mandates intermediaries to promptly remove or disable access to unlawful content upon receiving actual knowledge or notification from the government, without compromising evidence. Additionally, the Court noted that intermediaries lose protection under Section 79 if they have conspired, abetted, aided, or induced the commission of the unlawful act.

The Court also noted that Rule 11 of the POCSO Rules require persons in receipt of CSEAM being stored, possessed, distributed, circulated, transmitted, facilitated, propagated, or displayed or likely to be distributed, facilitated, transmitted in any manner, to report the contents to the SJPU or local police or cyber-crime portal (cybercrime.gov.in). In case such a person is an intermediary, Rule 11(2) further requires the intermediary to hand over the necessary material including the source from which the CSEAM may have originated. The report is required to include the details of the device in which the CSEAM was noticed and the suspected device from which such content was receiving including the platform on which content was displayed.

(b) Interplay with other reporting obligations

The Court observed that under a Memorandum of Understanding ("**MoU**") between the National Crime Records Bureau ("**NCRB**") and the US-based NGO National Centre for Missing & Exploited Children ("**NCMEC**"), social media intermediaries are required to report cases of child abuse to NCMEC, which forwards them to NCRB. The basis of this reporting is not centered on the POCSO or any other provision of Indian law. The Court observed that intermediaries have been found to comply only with the MoU and not with the local reporting obligations under POCSO. Further, the Court held that an intermediary cannot claim to have discharged its reporting obligation under Section 19 of POCSO and Rule 11 of the POCSO Rules by solely undertaking reporting as per the MoU.

The Court also noted that intermediaries cannot claim safe harbor under the IT Act unless they fulfill their due diligence duties, including reporting CSEAM to local authorities, as required by POCSO, and not just to the NCMEC. This duty goes beyond merely removing the content and includes prompt reporting to police.

Additionally, the Court urged the Parliament to amend Section 15(1) of POCSO to facilitate easier online reporting of CSEAM. It also emphasized that the term "child pornography" trivializes the crime, as it involves actual abuse, recommending the use of "child sexual exploitation and abuse material" instead.

Analysis and Conclusion

While the Court in the Just Rights Case has interpreted intermediaries' due diligence obligations under Section 79(2) of the IT Act to also include the reporting obligations on intermediaries under POCSO and POCSO Rules, the rationale for the same remain unclear. The due diligence obligations referred to in Section 79 of the IT Act are arguably those specifically issued by the Central Government under that provision, such as the IT Rules. It remains unclear how the Court has referred to a reporting obligation under an independent statutory scheme with independent consequences under POCSO to consequently also result in loss of safe harbour immunity.

Further, since the reporting obligation is triggered by the intermediary's knowledge, the question arises as to how intermediaries may be expected to have knowledge of CSEAM content on their platforms and to such extent will intermediaries be considered to have knowledge upon reporting of such content by users, or through their own proactive monitoring tools under Rule 4(4) of the IT Rules.

Given that NCMEC reporting will need to be supplemented with reporting to the Special Juvenile Police Unit, local police, or the national cybercrime portal as per POCSO, it appears that failure to do so may invite legal action (through FIRs or by initiating legal proceedings) by the NCPCR.

Global BigTech firms have raised concerns about the conflict between their exclusive reporting obligations under foreign laws. Based on reports, companies have highlighted that compliance with the Indian requirement may require formal agreements between Indian authorities and NCMEC.

Generative AI

The training of LLMs could also involve handling of CSEAM, due to indiscriminate scraping of publicly available internet data used to build training datasets. Additionally, in order to ensure that LLMs do not learn from, reproduce, or enable any form of CSEAM, companies also build safeguards in their training process, which involve data filtering and labelling of CSEAM. Such actions may inadvertently result in the unlawful storage or possession of CSEAM.

Given the wide language of Section 15 of POCSO which penalizes storage / possession of child pornography when carried out with specific intent / purpose and given the presumption of culpable mental state for offences under POCSO, there may be reporting obligations and liabilities for LLM developers under POCSO. Further, if the LLM generates CSEAM content, there may be exposure for liability under certain sections of the IT Act which are strict liability offences. In addition, if there is circulation/distribution or profiteering from CSEAM, there may also be potential exposure under BNS.

In the age of generative AI, these interpretations raise new questions such as how will developers, researchers, and platform operators navigate liability for unintentional exposure to, or generation of, illicit material? As courts extend legal definitions to include constructive possession and inchoate offences, clarity is needed on how these apply in technically

complex contexts like LLM training. Going forward, a nuanced approach must balance child protection imperatives with fair application of law in the Gen AI age.

Nishith Desai Associates - Karishma Karthik and HuzefaTavawalla